Безопасность информации ограниченного доступа при их автоматизированной обработке или без применения средств ВТ ,

Вопросы нормативно-методического обеспечения

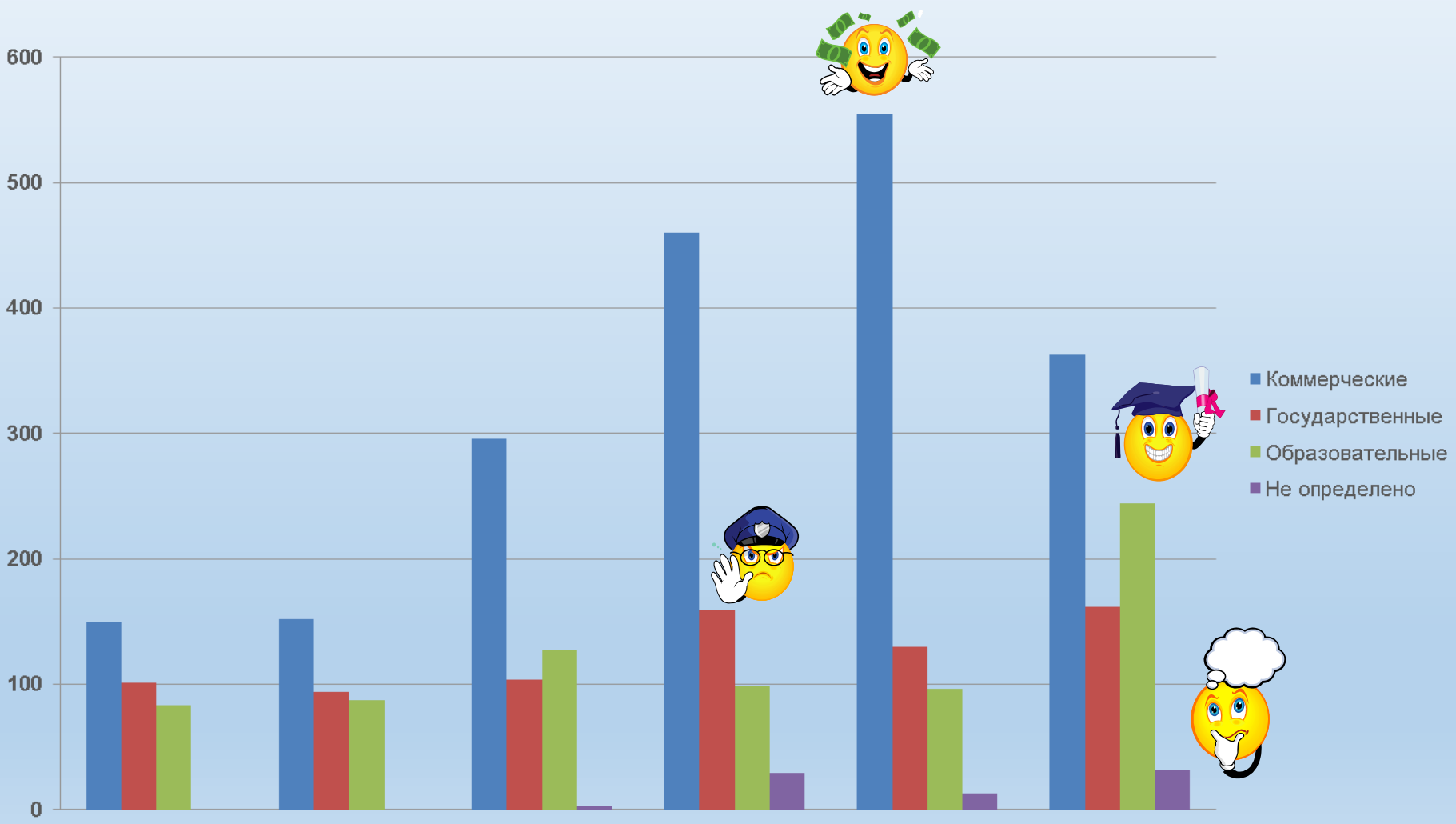
Организационно-правовые основы технической защиты информации

Актуальность проблемы обеспечения безопасности персональных данных

«Кто владеет информацией – тот владеет миром...»

сэр У. Черчиль

По типам организаций



Общая статистика

Аналитическим центром InfoWatch зарегистрировано 1395 (3,8 в день,
116 в месяц) случаев утечки информации. В результате утечек скомпрометировано 767 млн персональных данных (записей ПДн), – номера социального страхования, реквизиты пластиковых карт, иная критически важная информация (см. Рисунок 1).

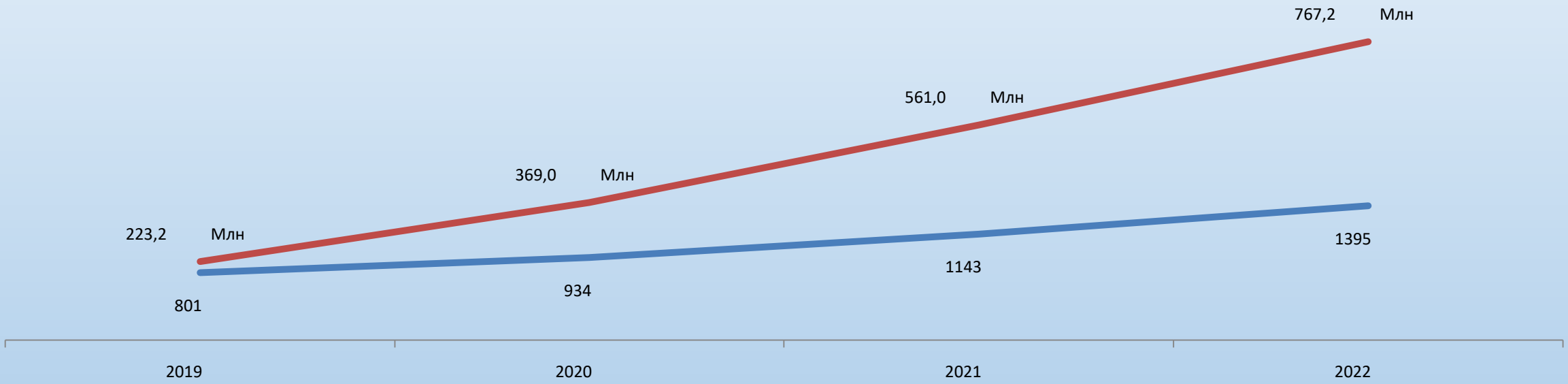


Рисунок 1. Число утечек информации и объем утекших записей ПДн, скомпрометированных в результате утечек.

Аналитический центр InfoWatch наряду с утечками, причиной которых стали внутренние нарушители, регистрирует утечки информации, причиной которых стали внешние воздействия – целевые атаки и проч., повлекшие компрометацию данных.

Только горячие цифры

Обнародовано (в СМИ и иных источниках) и зарегистрировано Аналитическим центром InfoWatch случаев утечки конфиденциальной информации, что на **треть** превышает число утечек, зарегистрированных в предыдущем году году.

 Больше всего утечек информации связано с персональными данными – в **92%** случаев утекала именно эта информация. Более **767 млн** персональных данных были скомпрометированы из-за ошибок или намеренных действий внутренних нарушителей, вследствие внешних атак (кибер-атаки и намеренные утечки от внутренних и внешних нарушителей).

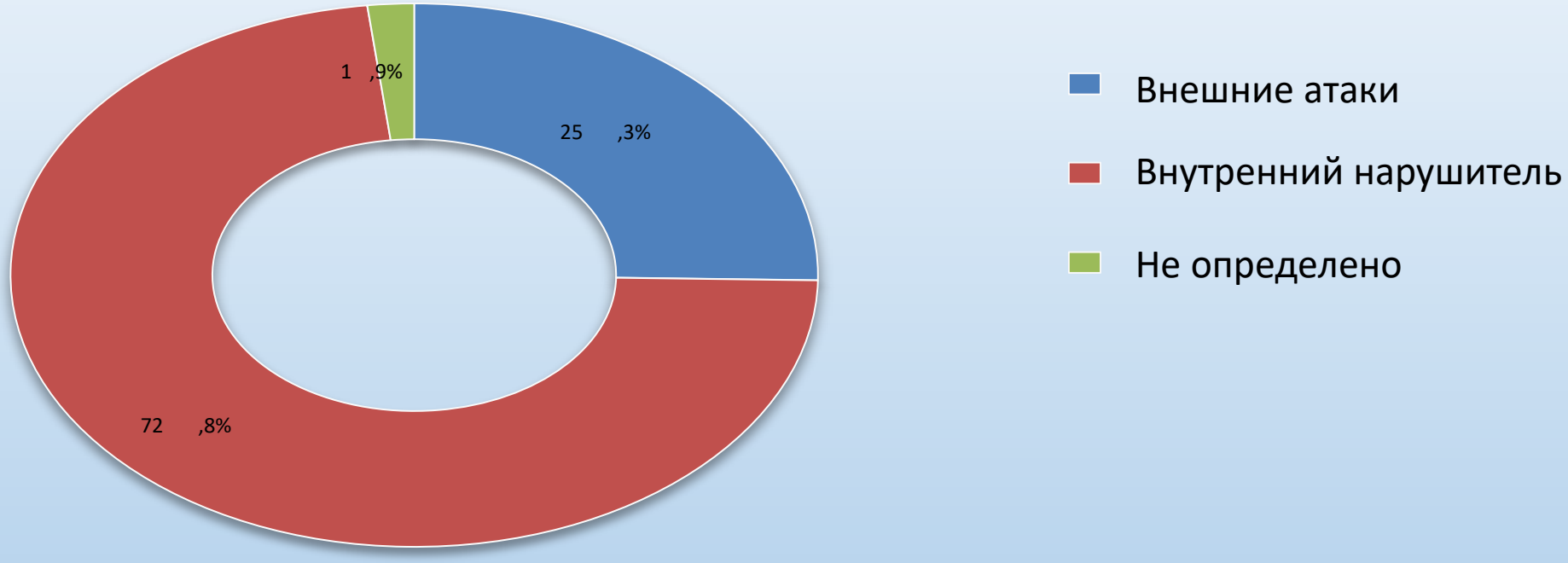
 В результате каждой «утекло» более **10 млн** персональных данных. На «мега-утечки» пришлось **89%** всех скомпрометированных записей.

 Банки, наряду с интернет-сервисами, ретейлерами, образовательными и медицинскими учреждениями, являются основным источником утечек персональных данных.

 В более, чем **половине** случаев виновными в утечке информации оказались сотрудники компаний. В **1%** случаев – высшие руководители организаций.

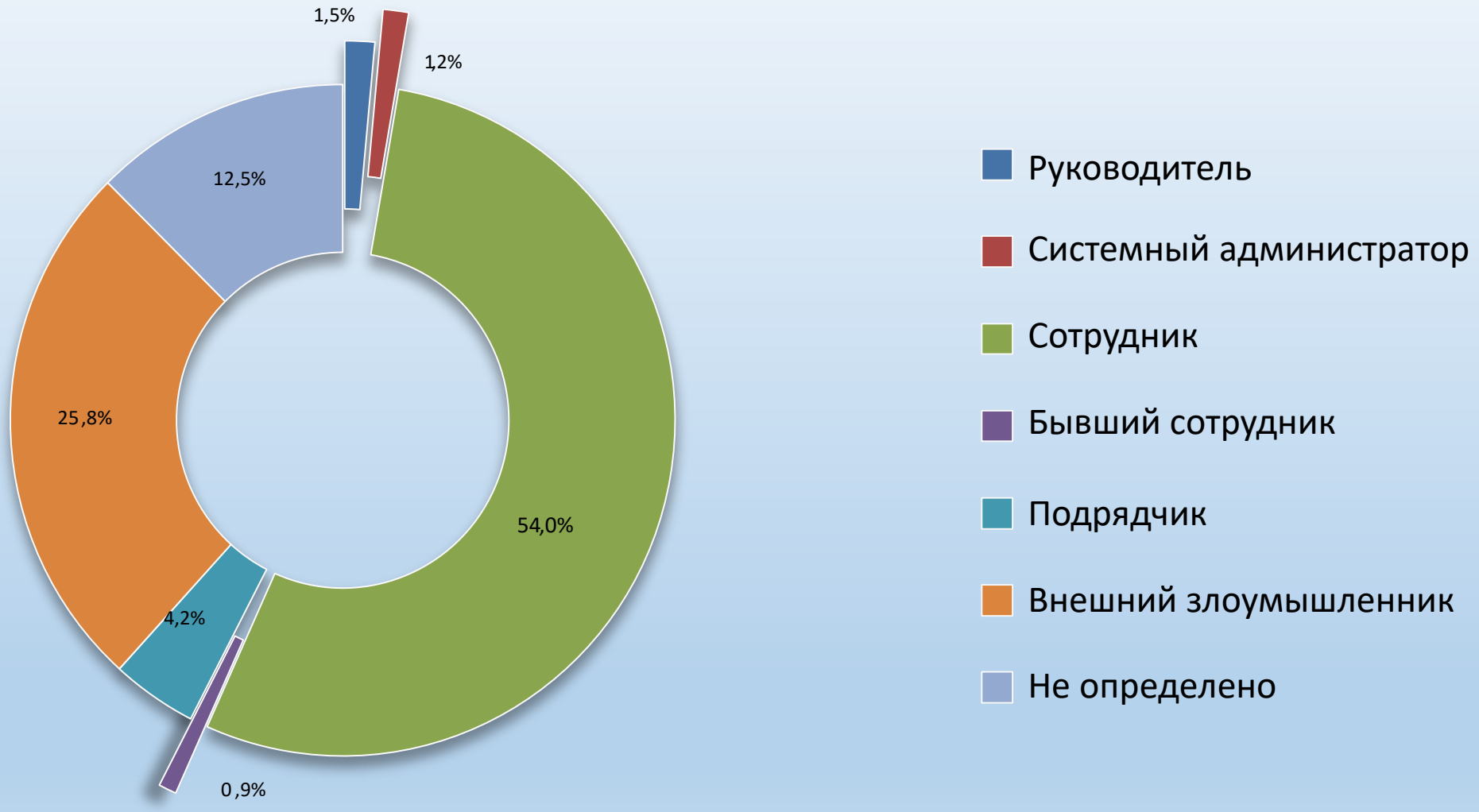
 Россия заняла второе место по числу известных утечек. В исследуемый период зарегистрировано **167** случаев утечки конфиденциальной информации из российских компаний и государственных организаций. «**мерОбщая**

Распределение утечек по вектору воздействия.

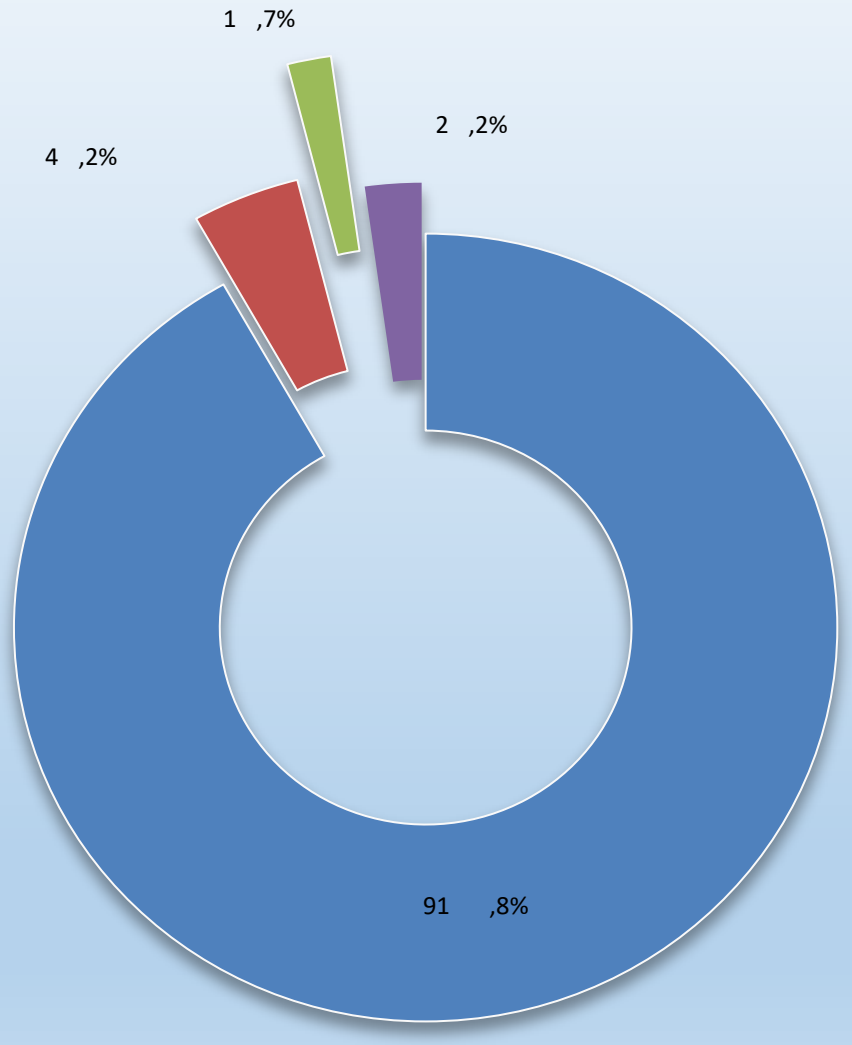


В результате воздействия **внутреннего нарушителя** скомпрометировано **350 млн персональных данных (0,34 млн на утечку).**
Итогом внешнего воздействия стала компрометация **410 млн записей (1,16млн на утечку)**.

Доля в распределении по виновнику утечки

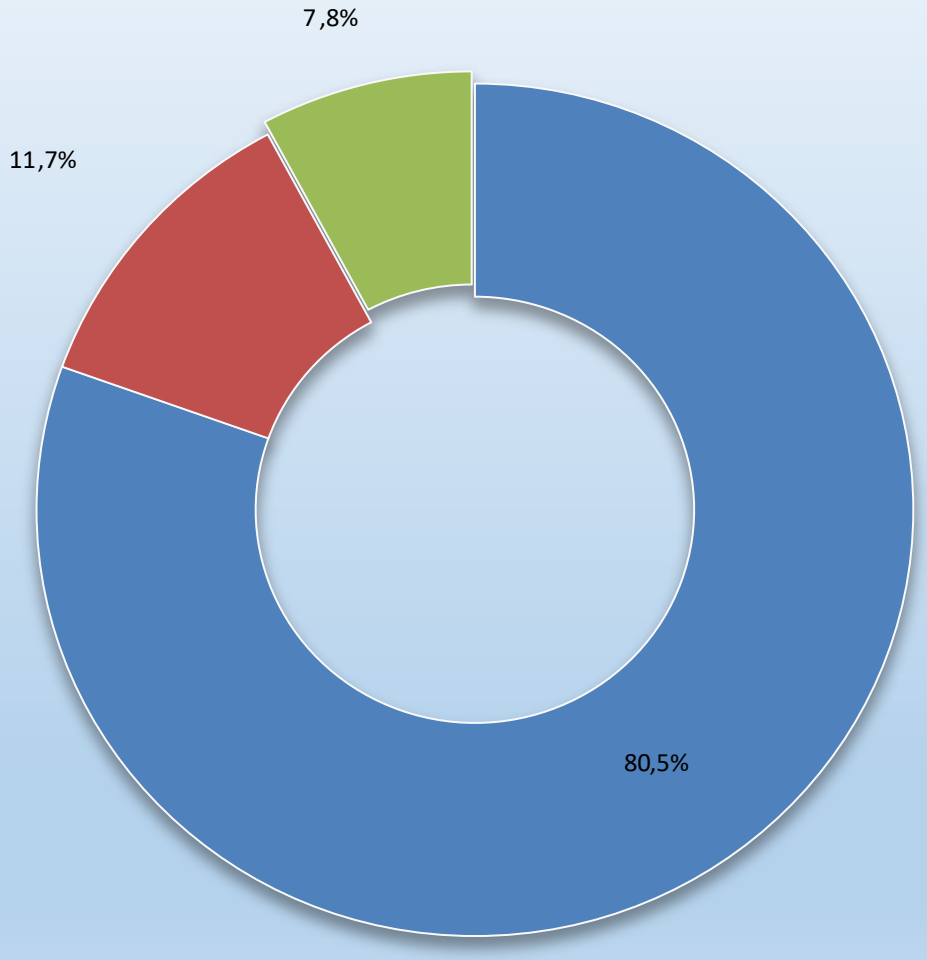


Распределение утечек по типам данных.



- Персональные данные и платежная информация
- Коммерческая тайна, know-how
- Государственная тайна
- Не определено

По характеру действий нарушителя

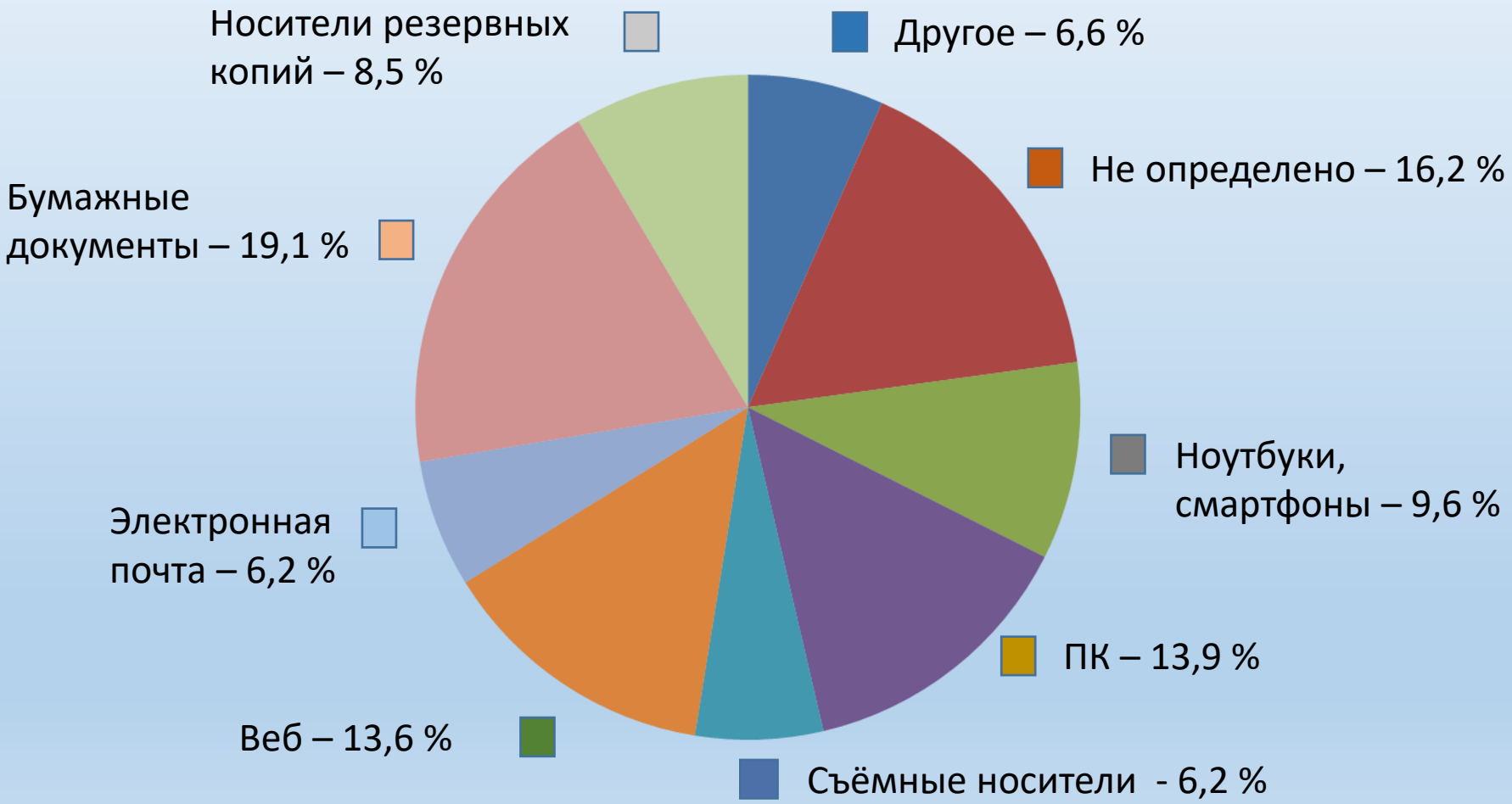


- **Утечка информации**
- **Мошенничество с использованием данных**
- **Превышение прав доступа**

Вывод:

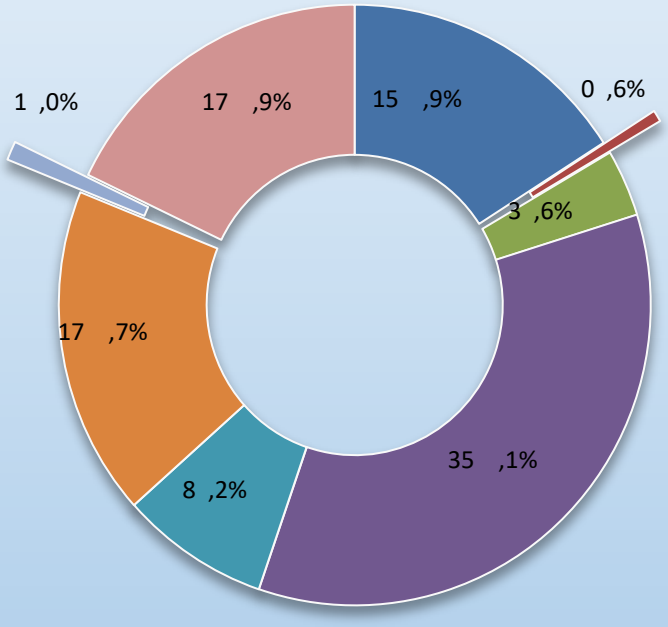
1. *Прирост объема скомпрометированных персональных данных происходит за счет «мега-утечек».*
2. *Прирост числа утечек спровоцирован в большей степени внешними атаками.*
3. *Основные показатели, отражающие глобальную картину утечек данных – динамика роста утечек.*
4. *Доля персональных данных и коммерческой тайны, доля сотрудников в распределении по виновнику утечки – практически не изменяются год к году.*
5. *Доля утечек неопределенной природы последовательно снижается.*

Каналы утечек (2012 г)

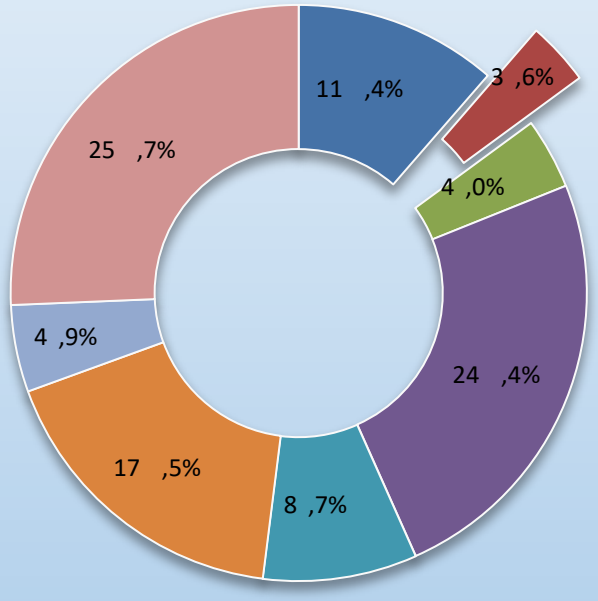


http://www.infowatch.ru

Каналы утечек



- Кража/потеря оборудования
- Мобильные устройства
- Съемные носители
- Сеть (браузер, Cloud)
- Электронная почта
- Бумажные документы
- IM (текст, голос, видео)
- Не определено

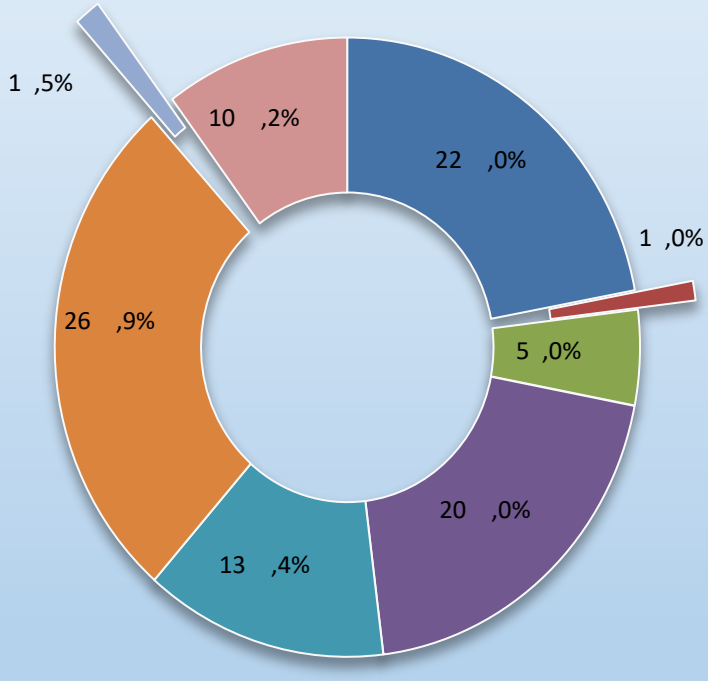


2021

2022

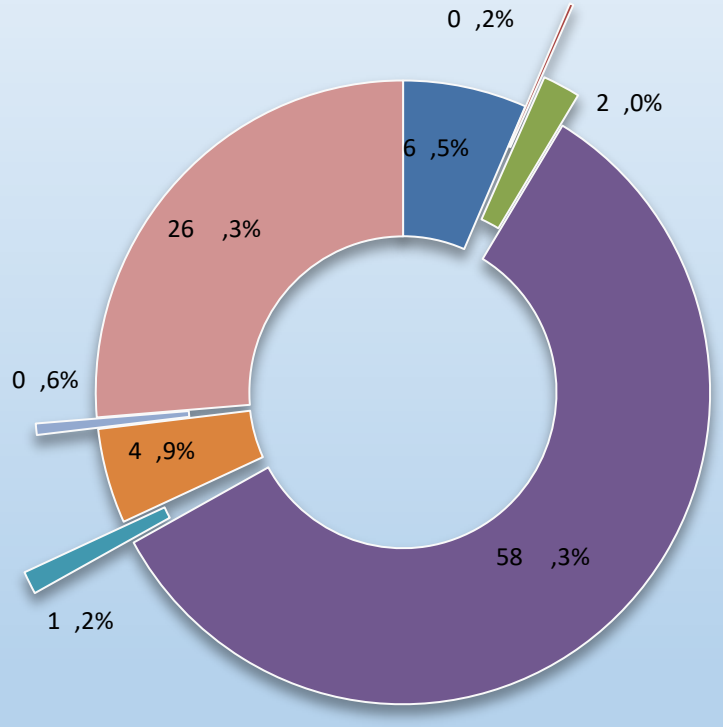
Распределение случайных и умышленных утечек

Случайные



- Кража/потеря оборудования
- Мобильные устройства
- Съемные носители
- Сеть (браузер, Cloud)
- Электронная почта
- Бумажные документы
- IM (текст, голос, видео)
- Не определено

Умышленные



Обобщенная модель способов овладения конфиденциальной информацией

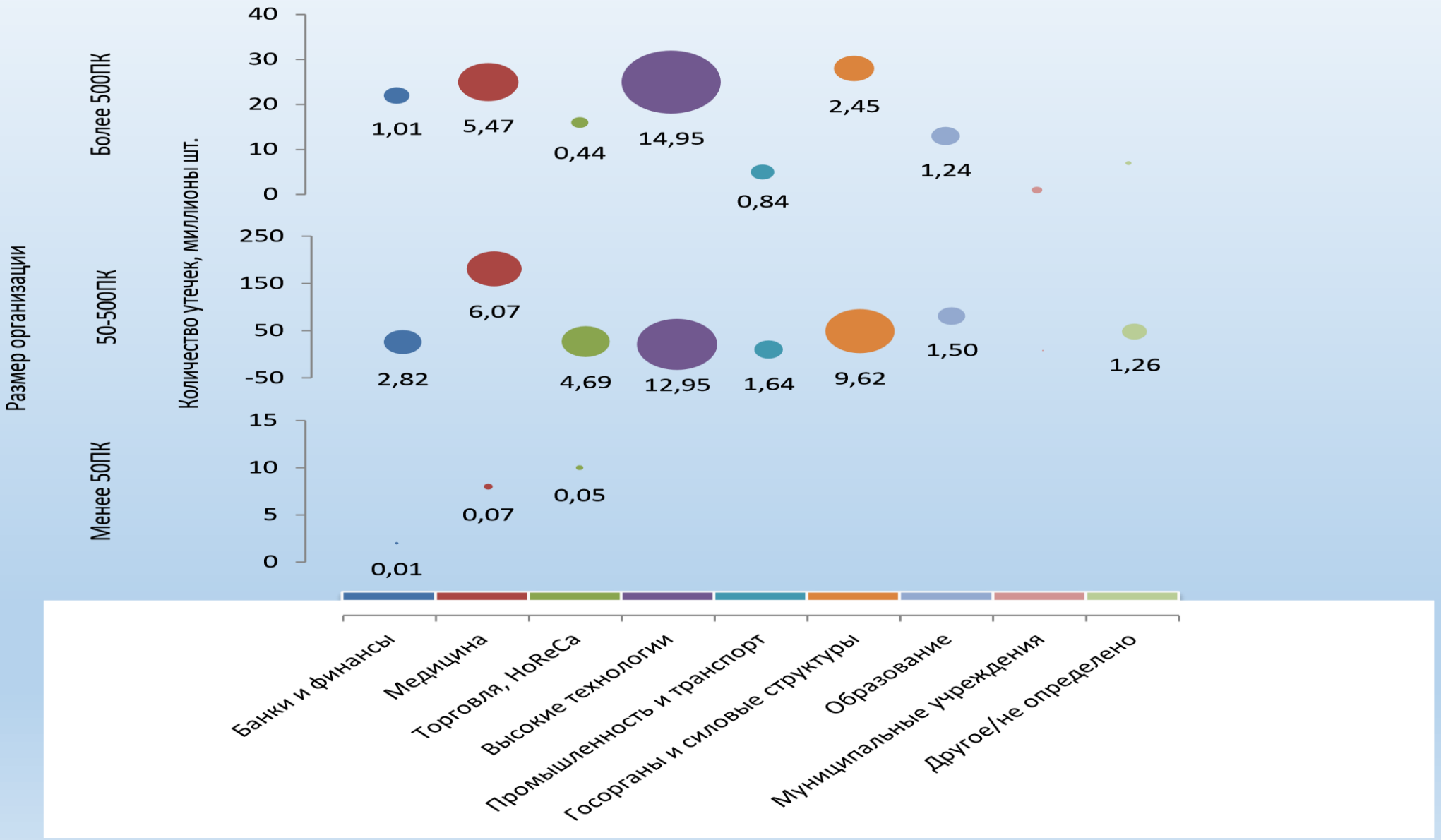
№ п/п	Источники	СПОСОБЫ													Общее количество по источнику
		инициативное сотрудничество	склонение к сотрудничеству	выпытывание	подслушивание	наблюдение	хищение	копирование	подделка (модификация)	уничтожением (порча, разрушение)	незаконное подключение	перехват	незаконное ознакомление	фотографирование	сбор и аналитическая обработка	
1.	Люди	■	■	■	■	■	■		■	■			■	■		10
2.	Документы					■	■	■	■	■		■	■	■	■	9
3.	Публикации								■				■		■	3
4.	Технические носители						■	■	■	■					■	5
5.	ТСПИ				■	■	■	■	■	■	■	■	■	■		10
6.	Продукция					■	■	■	■	■			■	■		7
7.	Отходы						■								■	2
Итого		1	1	1	2	4	6	4	6	5	1	2	5	4	4	46

Вывод:

1.Существенное различие в распределении умышленных и случайных утечек по каналам говорит о ***растущей квалификации внутреннего нарушителя****.*

*2.Утечек данных по «****традиционным****» каналам фиксируется все меньше, так как злоумышленники их не используют, поскольку* ***хорошо осведомлены*** *о функциональных возможностях защитных решений.*

Отраслевая карта утечек



Вывод:

*1.Ситуация с защитой **персональных данных** в компаниях далека от идеальной.*

*2.В большей степени это касается **среднего бизнеса**, где утечки данных происходят чаще, чем в крупных компаниях. Причем большая часть утечек в среднем бизнесе пришлась на случайные.*

*3.В 2014 году компании среднего размера заняли главенствующее положение в ряду «поставщиков» конфиденциальной информации. В этом аспекте особенно «отличились» **интернет-сервисы**, **образовательные** и **медицинские** учреждения. Именно эти организации обладают наибольшим количеством персональных данных и не спешат их защищать, поскольку **не несут прямых финансовых потерь**.*

*** Причина такого положения небольших и средних компаний объясняется тем, что на рынке практически полностью отсутствуют эффективные и недорогие средства защиты информации, ориентированные на СМБ-сегмент.**

Основные нарушения требований 152-ФЗ

- несоответствие сведений, указанных в уведомлении, фактической деятельности Оператора
- обработка персональных данных без согласия субъектов персональных данных
- несоответствие содержания письменного согласия субъекта на обработку его персональных данных требованиям Федерального закона
- непринятия мер по исключению НСД к обрабатываемым персональным данным при неавтоматизированной обработке

Актуальность проблемы

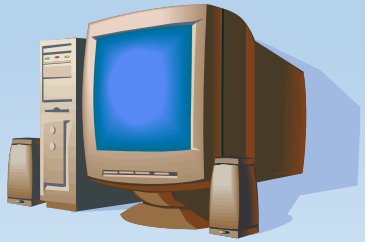
- значительное увеличение правонарушений, связанных с утечками информации в организациях (компаниях)
- появление новых угроз и уязвимостей
- стремление Государства регламентировать деятельность по защите информации
- отсутствие единого понимания отдельными представителями бизнеса, проблемы защиты информации
- неоднозначная трактовка некоторых положений нормативных документов ФСТЭК и ФСБ
- увеличение тяжести последствий утечки информации
- появление технологий, позволяющих правонарушителям воспользоваться полученной информацией
- **Информация стала объектом торга**

Основные понятия в области технической защиты информации
И
10 самых распространённых ошибок персонала при работе с КИ

Информация - сведения (сообщения, данные) независимо от формы их представления

- акустическая (речевая) информация
- видовая информация
- информация, обрабатываемая (циркулирующая) в ИС, в виде электрических, электромагнитных, оптических сигналов;

- информация, обрабатываемая в ИС, представленная в виде бит, байт, IP-протоколов, файлов и других логических структур.



149-ФЗ от 27 июля 2006 года

Термины и определения

Конфиденциальность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

Доступность информации - состояние информации, характеризуемое способностью АС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Целостность информации – состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки и хранения.

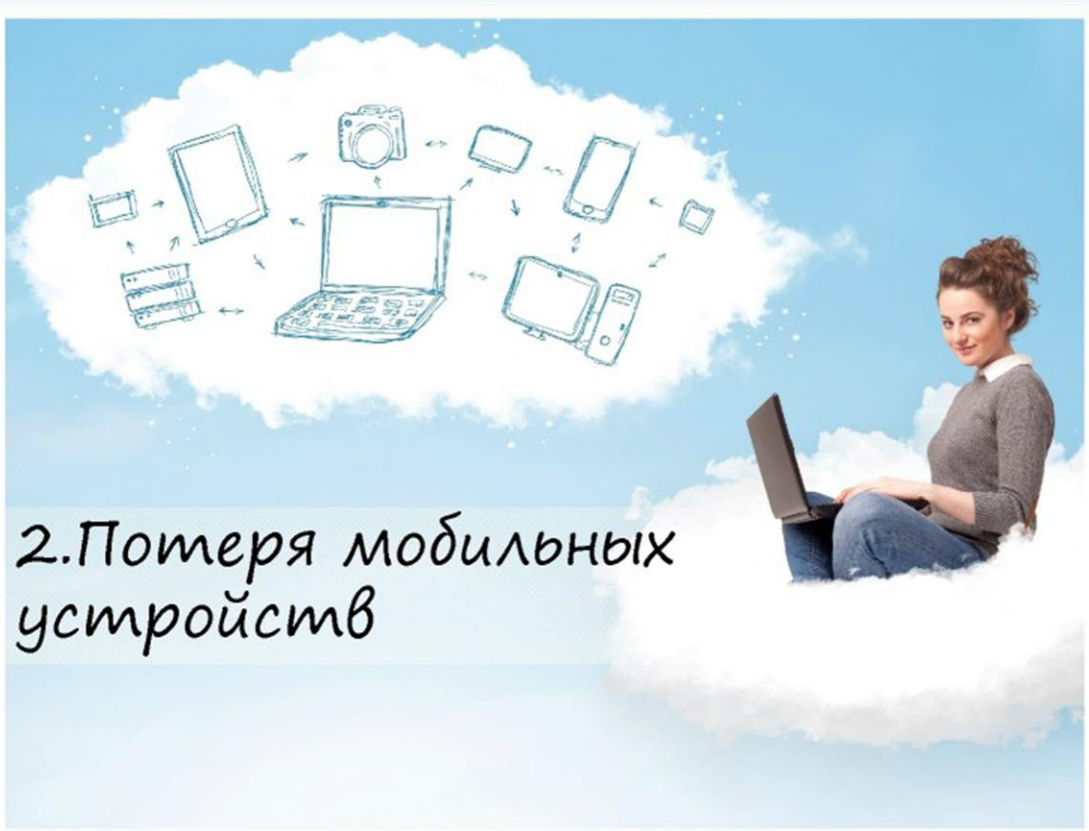
10 наиболее распространенных ошибок персонала

http://www.infowatch.ru

10 наиболее распространенных ошибок персонала

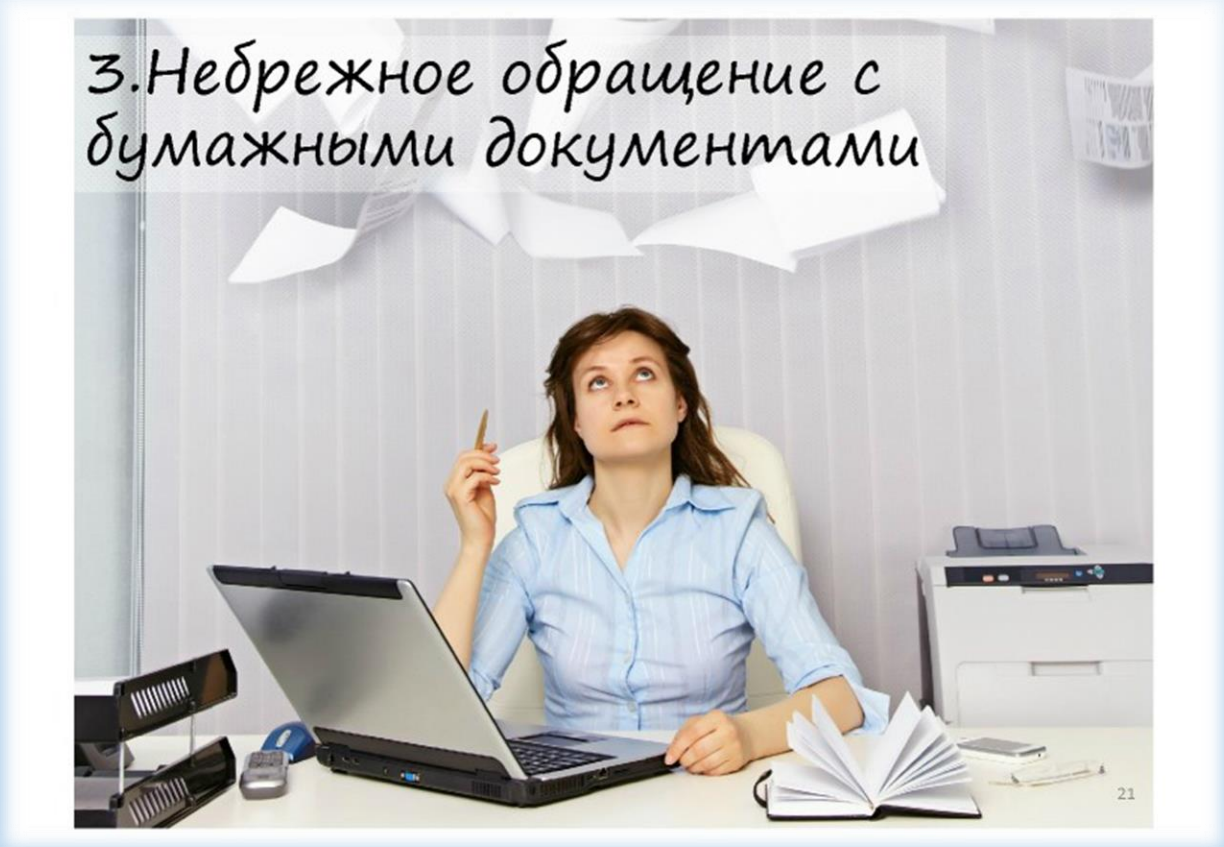
http://www.infowatch.ru

10 наиболее распространенных ошибок персонала



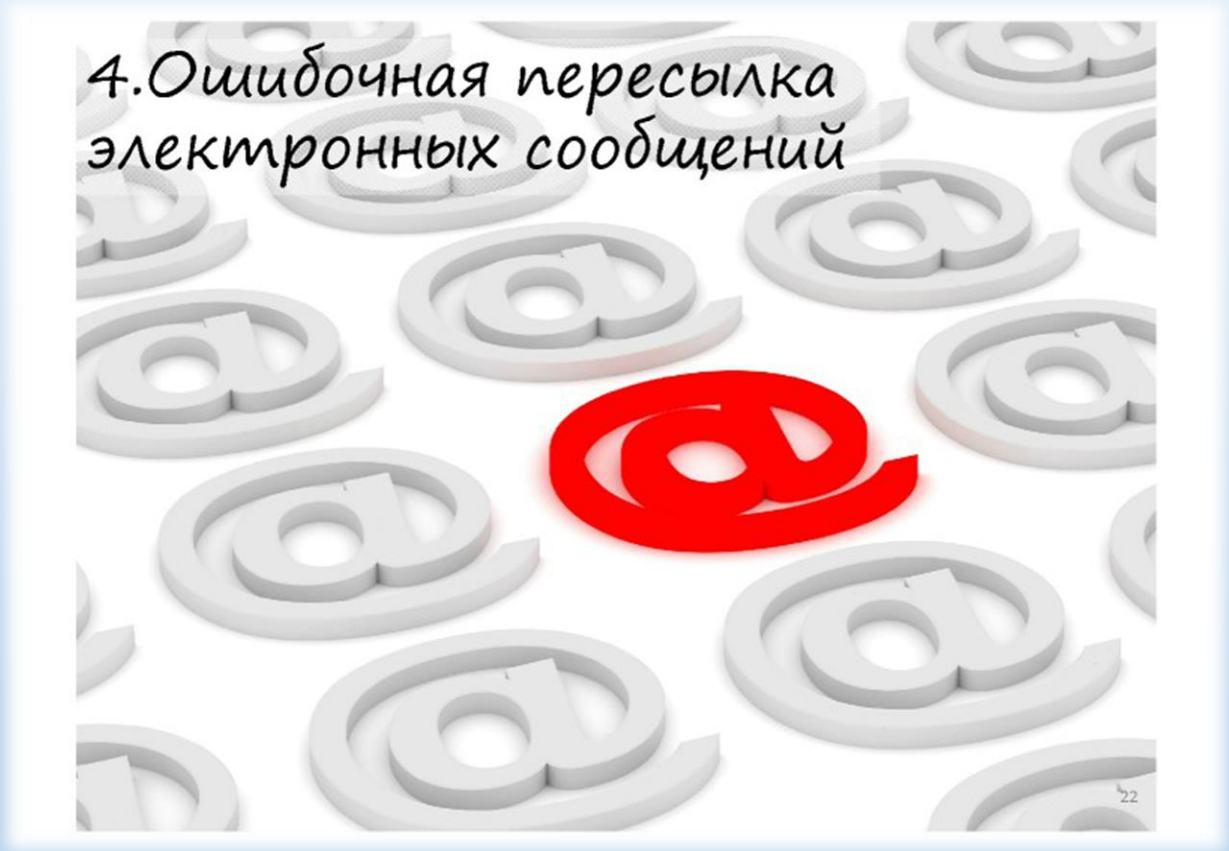
http://www.infowatch.ru

10 наиболее распространенных ошибок персонала



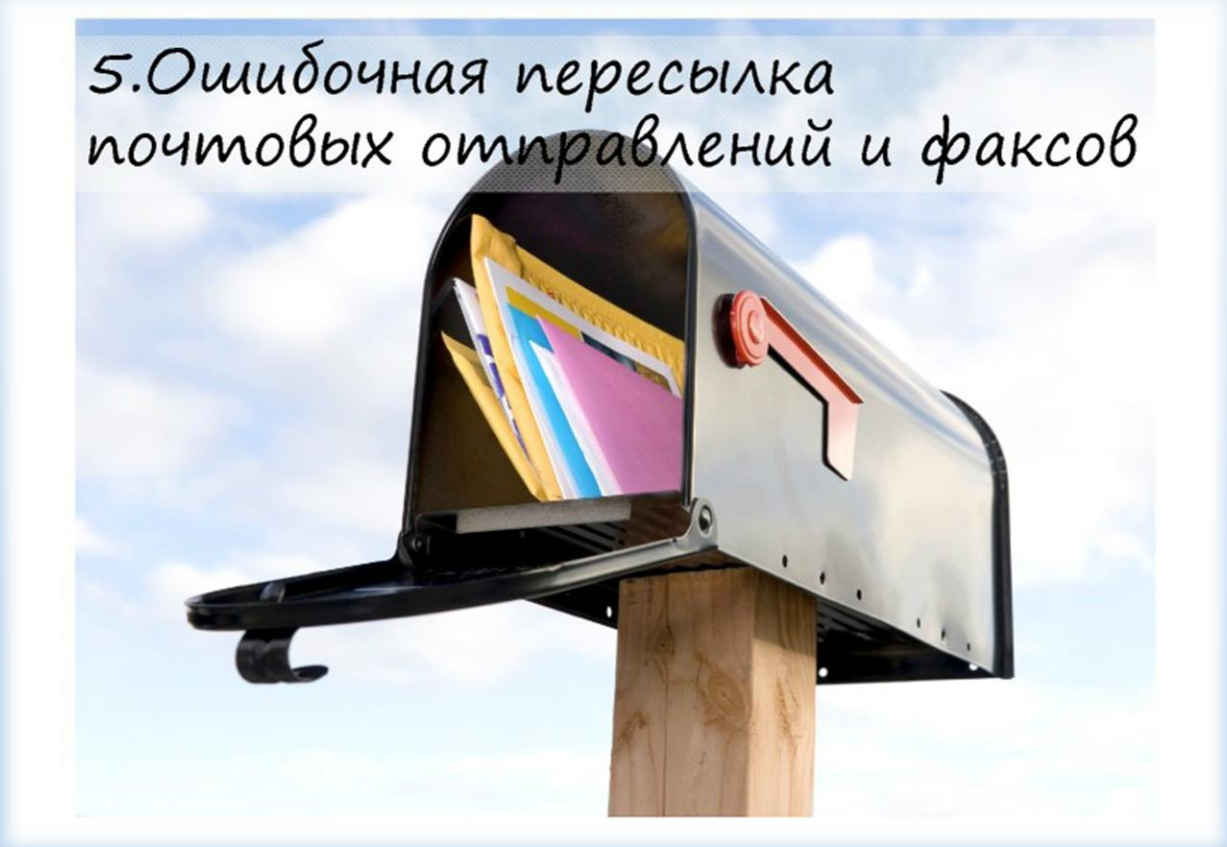
http://www.infowatch.ru

10 наиболее распространенных ошибок персонала



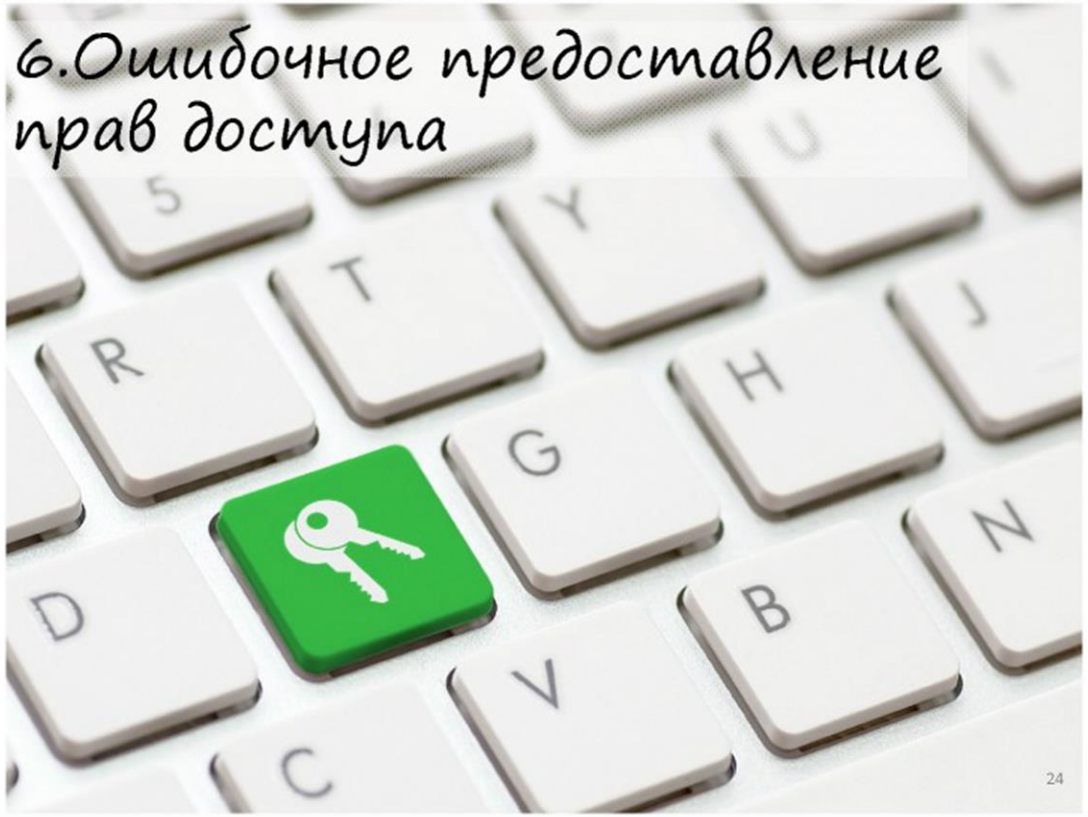
http://www.infowatch.ru

10 наиболее распространенных ошибок персонала



http://www.infowatch.ru

10 наиболее распространенных ошибок персонала

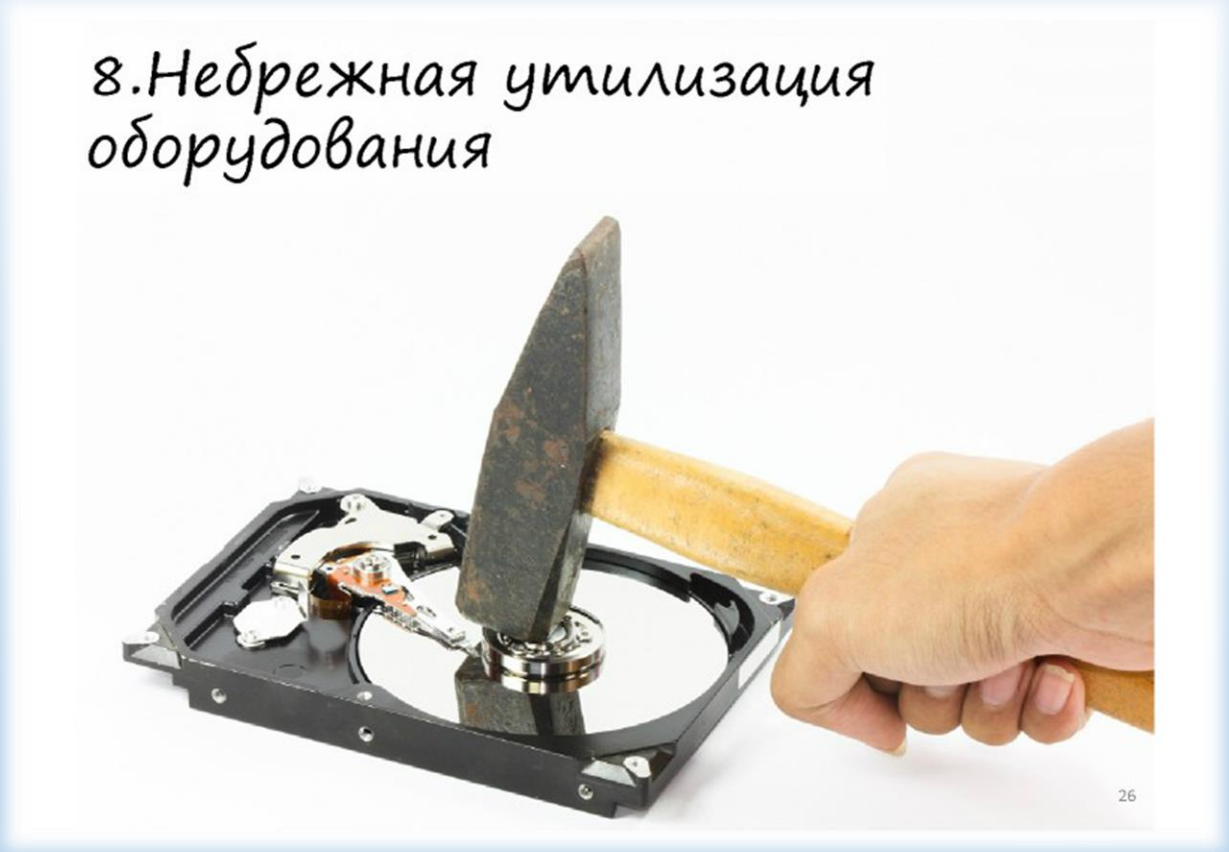


http://www.infowatch.ru

10 наиболее распространенных ошибок персонала

http://www.infowatch.ru

10 наиболее распространенных ошибок персонала

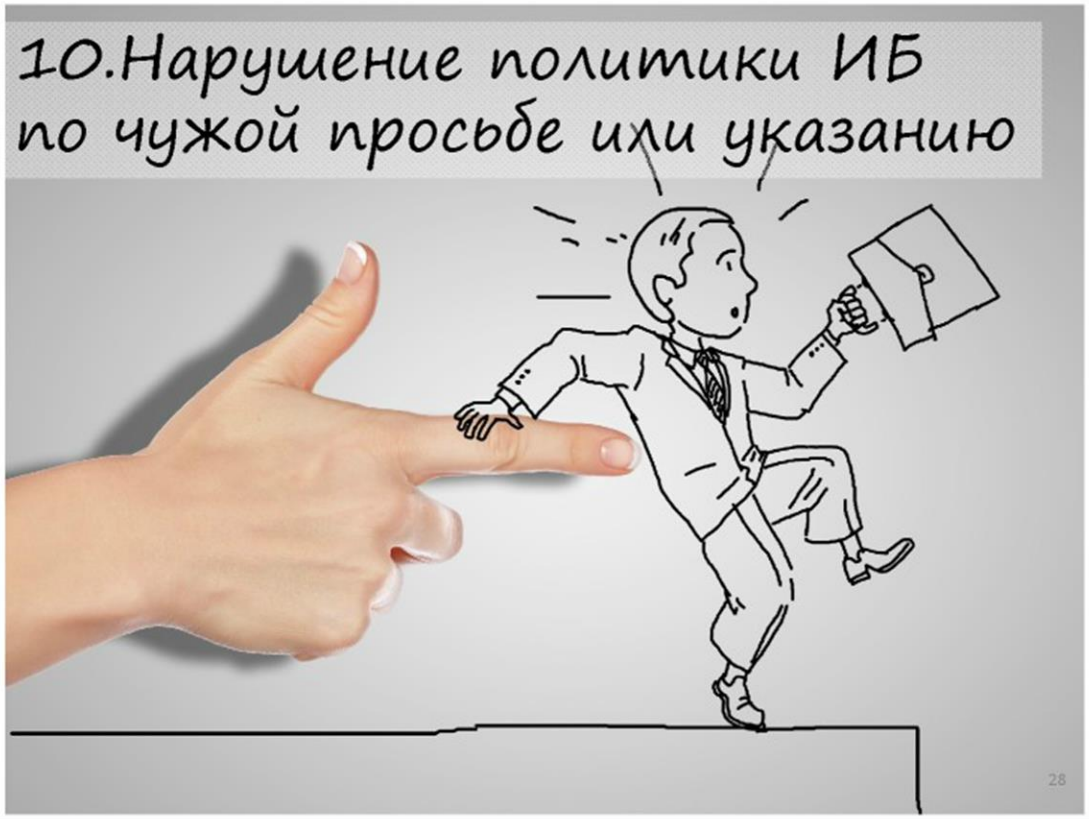


http://www.infowatch.ru

10 наиболее распространенных ошибок персонала

http://www.infowatch.ru

10 наиболее распространенных ошибок персонала



http://www.infowatch.ru

10 наиболее распространенных ошибок персонала

10 ошибок сотрудников

INFOWATCH

1. Потеря съемных носителей
2. Потеря мобильных устройств (в т.ч. в результате кражи)
3. Небрежное обращение с бумажными документами
4. Ошибочная пересылка электронных сообщений
5. Ошибочная пересылка почтовых отправлений и факсов
6. Ошибочное предоставление прав доступа, выкладывание закрытой информации в общий доступ
7. Небрежная утилизация бумажных документов
8. Небрежная утилизация оборудования
9. Передача оборудования, содержащего информацию ограниченного доступа, на техническое обслуживание третьим лицам
10. Нарушение политики безопасности по просьбе других сотрудников и прочих лиц (социальная инженерия)

http://www.infowatch.ru

Нарушение конфиденциальности

Перехват – получение несанкционированного доступа к ресурсу.

- Подключение к кабелю связи с целью перехвата данных
- Незаконное копирование файлов и программ

Нарушение целостности

Модификация – открытие несанкционированного доступа к ресурсу и его изменение нарушителем.

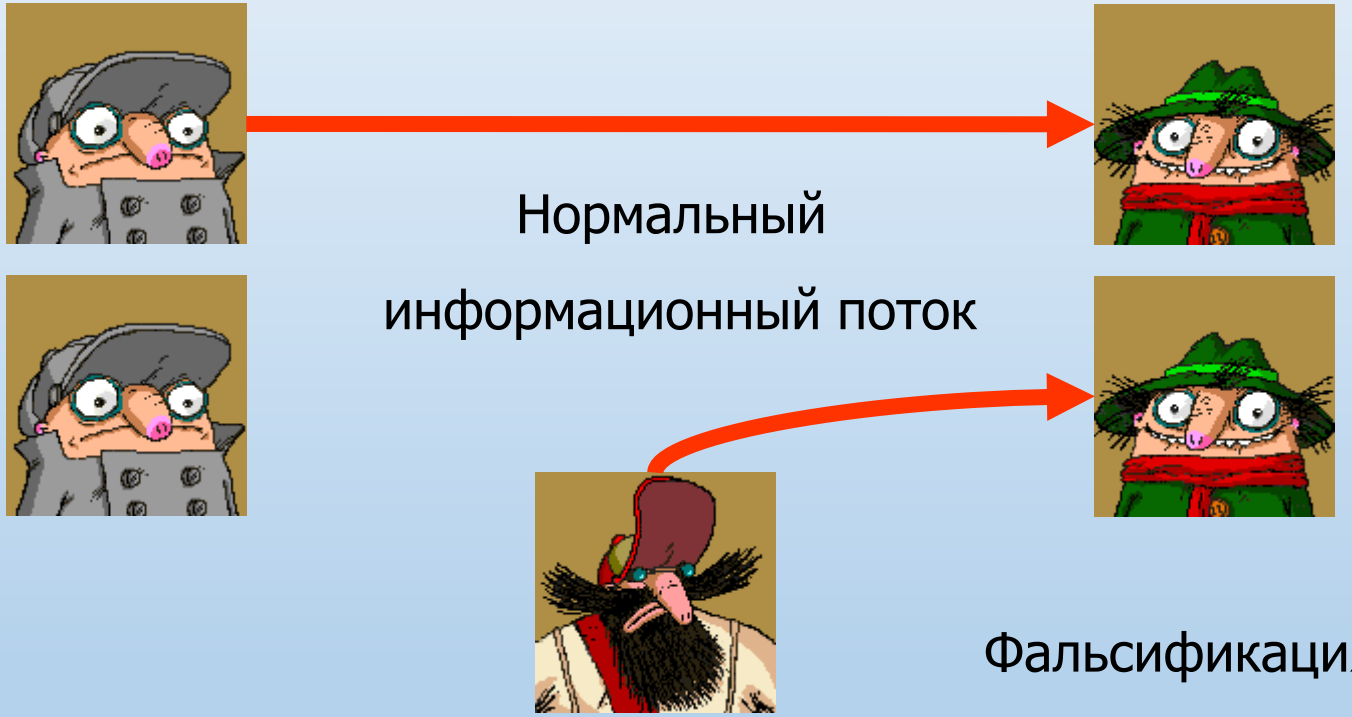
- Изменение значений в файле данных
- Модификация кода программы с целью изменения ее функций
- Изменение содержимого передаваемого по сети сообщения

Нарушение доступности

Разъединение – уничтожение ресурса системы, либо приведение его в состояние недоступности или негодности.

- Вывод из строя оборудования
- Обрыв линии связи
- Разрушение файловой системы

Нарушение аутентичности



Фальсификация – внесение в систему ложного объекта.

- Отправка поддельных сообщений по сети
- Добавлений записей в файл

Термины и определения

информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов

информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

информационно - телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники

149-ФЗ от 27 июля 2006 года

Термины и определения

обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам

149-ФЗ от 27 июля 2006 года

Термины и определения

доступ к информации - возможность получения информации и ее использования

предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц

распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц

149-ФЗ от 27 июля 2006 года

Термины и определения

электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети

документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель

электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах

149-ФЗ от 27 июля 2006 года

Информационная безопасность - механизм защиты, обеспечивающий:

- конфиденциальность: доступ к информации только авторизованных пользователей;
- целостность: достоверность и полноту информации и методов ее обработки;
- доступность: доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

ГОСТ Р ИСО/МЭК 17799-2005

Информационная безопасность - это защита информации от широкого спектра угроз с целью:

- обеспечения непрерывности бизнеса
- минимизации рисков бизнеса
- максимального увеличения возврата инвестиций и возможностей бизнеса

ISO/IEC 27002-2005

Термины и определения

Оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

149-ФЗ от 27 июля 2006 года

Оператор

- государственный орган
- муниципальный орган
- юридическое лицо
- физическое лицо

совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с персональными данными

152-ФЗ от 27 июля 2006

Термины и определения

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

Перечни запрашиваемых ПДн определяются

75 международными правовыми актами

13 кодексами РФ

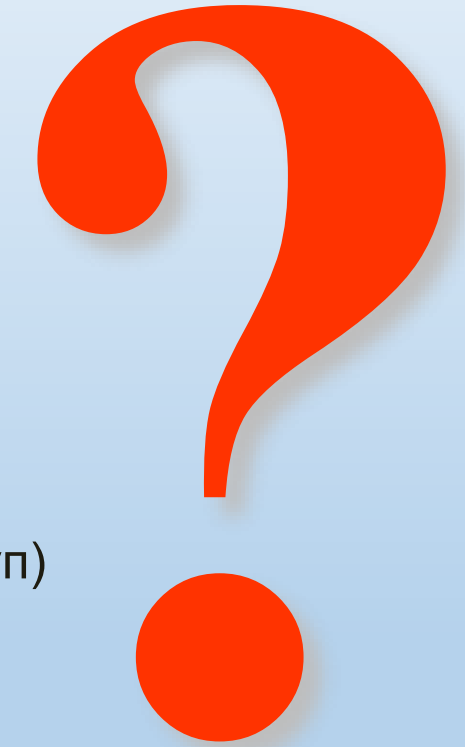
100 федеральными законами

250 актами Правительства РФ

152-ФЗ от 27 июля 2006

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными

- сбор
- запись
- систематизация
- накопление
- хранение
- уточнение (обновление, изменение)
- извлечение
- использование
- передача (распространение, предоставление, доступ)
- обезличивание
- блокирование
- удаление
- уничтожение



152-ФЗ от 27 июля 2006

Термины и определения

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники (СВТ)

СВТ - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем

Блокирование персональных данных - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения персональных данных)

152-ФЗ от 27 июля 2006

Термины и определения

Уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание персональных данных в ИСПДн и (или) в результате которых уничтожаются материальные носители персональных данных

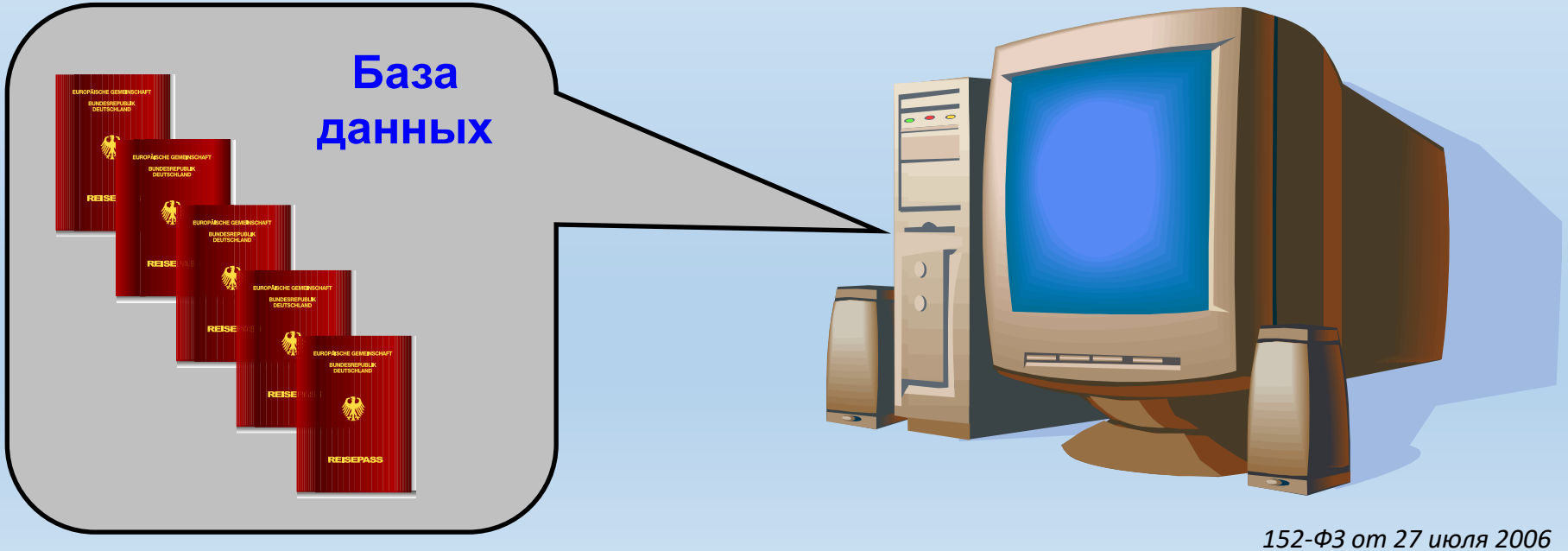
Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту персональных данных

Трансграничная передача ПДн - передача персональных данных оператором через Государственную границу РФ органу власти иностранного государства, физическому или юридическому лицу иностранного государства

152-ФЗ от 27 июля 2006

Термины и определения

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств



152-ФЗ от 27 июля 2006

Термины и определения

Техническая защита конфиденциальной информации (ТЗКИ) - защита информации некриптографическими методами, направленными на предотвращение утечки защищаемой информации:

- по техническим каналам
- от несанкционированного доступа к ней
- от специальных воздействий на информацию

Термины и определения

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

п.2 постановления Правительства Российской Федерации от 17 ноября 2007 года №781

Термины и определения

Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Защищаемые помещения (ЗП) - помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

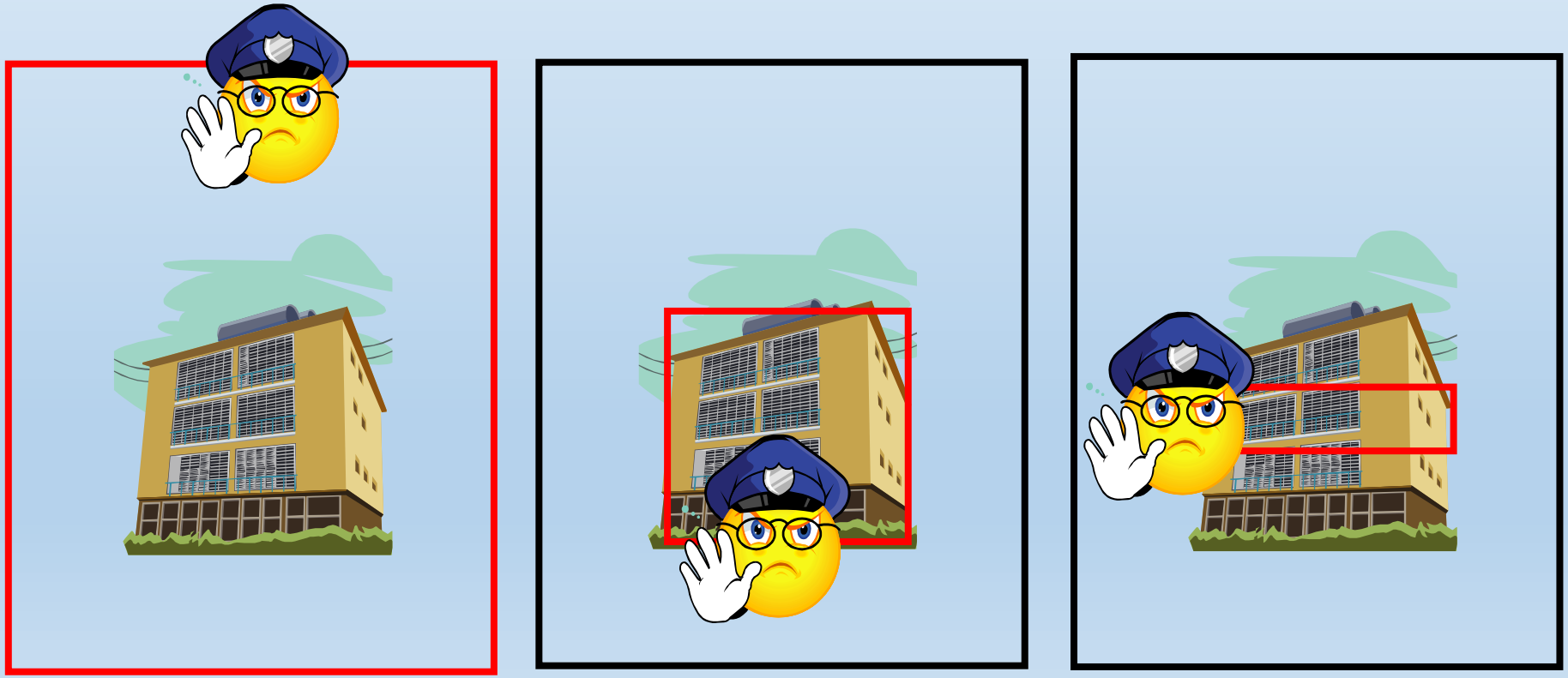
Термины и определения

Основные технические средства и системы (ОТСС) - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации

Вспомогательные технические средства и системы (ВТСС) - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, размещаемые совместно с ОТСС или в ЗП

Термины и определения

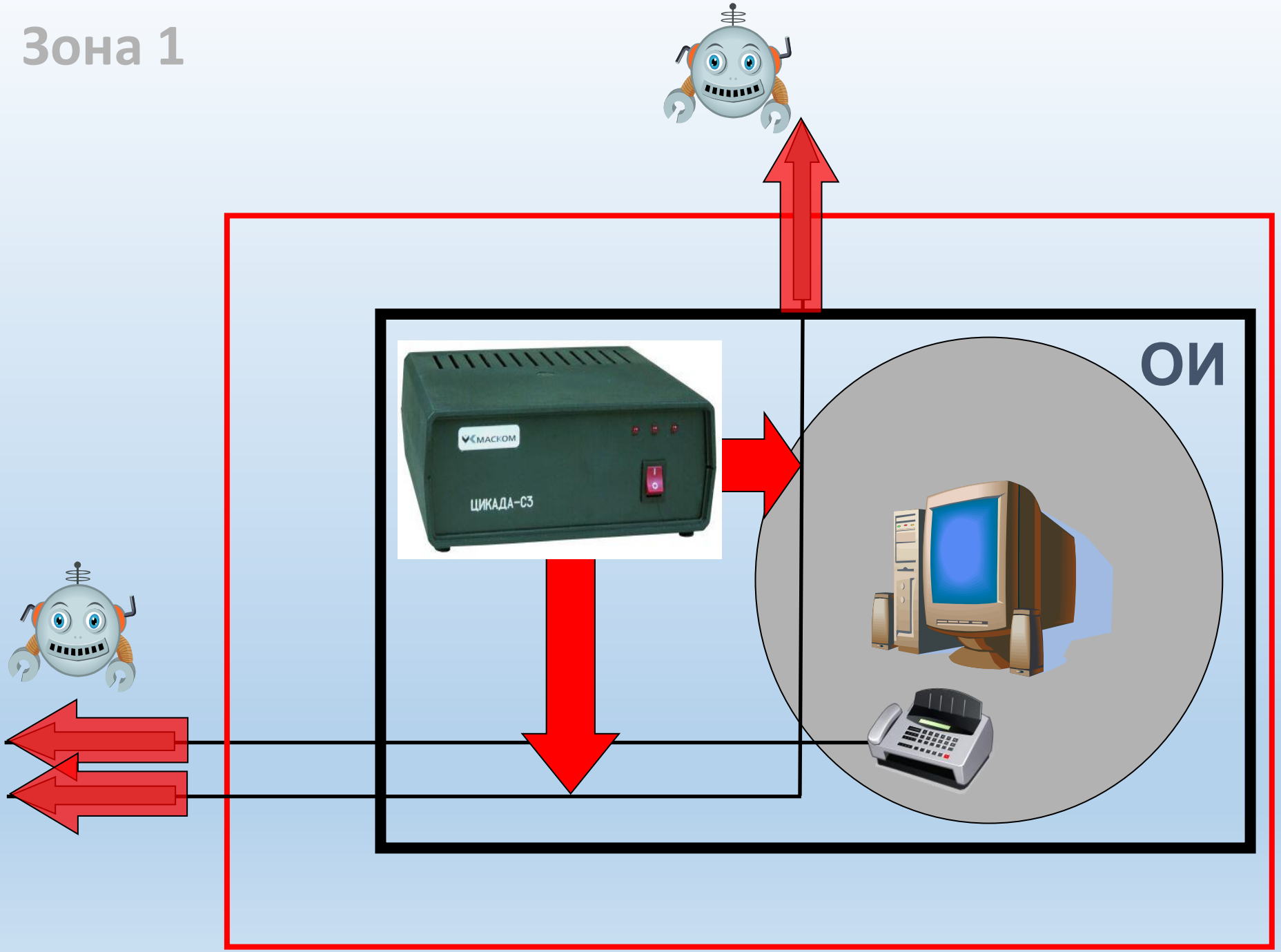
Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.



Зона 1

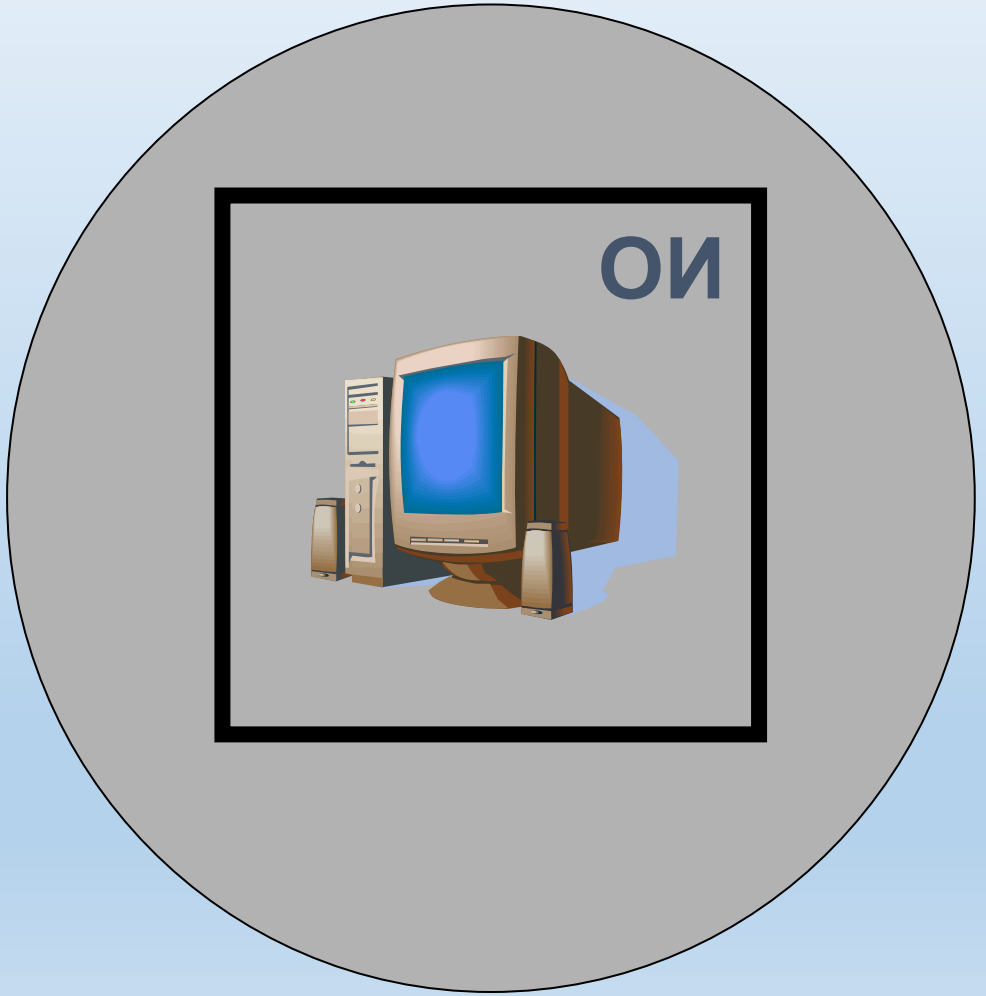
Пространство вокруг ОТСС, на границе и за пределами которого уровень наведенного от ОТСС сигнала в ВТСС, а также в посторонних проводах и линиях передачи информации, имеющих выход за пределы КЗ, не превышает нормированного значения.

Зона 1

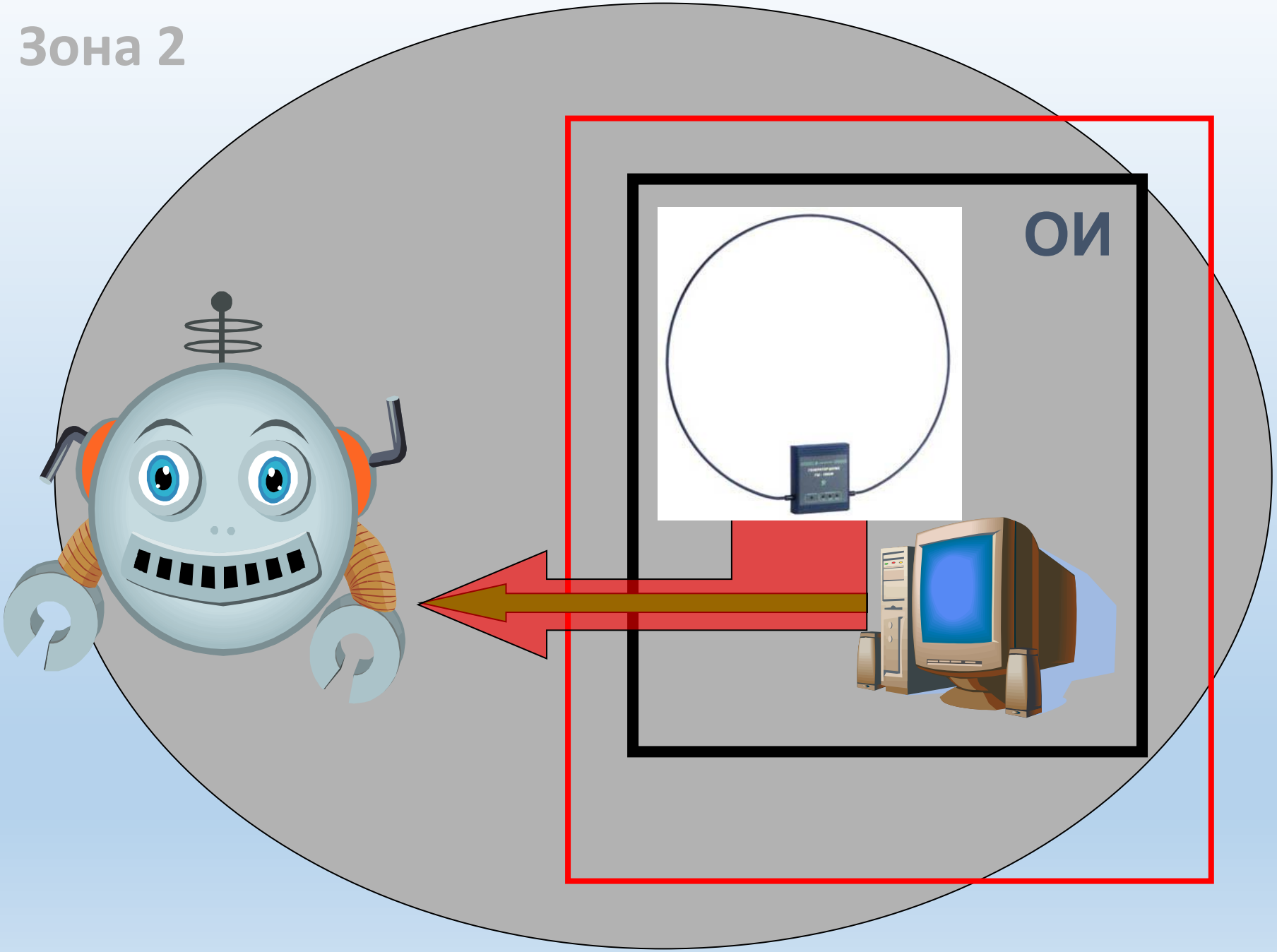


Зона 2

Пространство вокруг ОТСС на границе и за пределами которого напряженность электромагнитного поля информативного сигнала не превышает нормированного значения.



Зона 2



Термины и определения

Доступ к информации (доступ) - ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

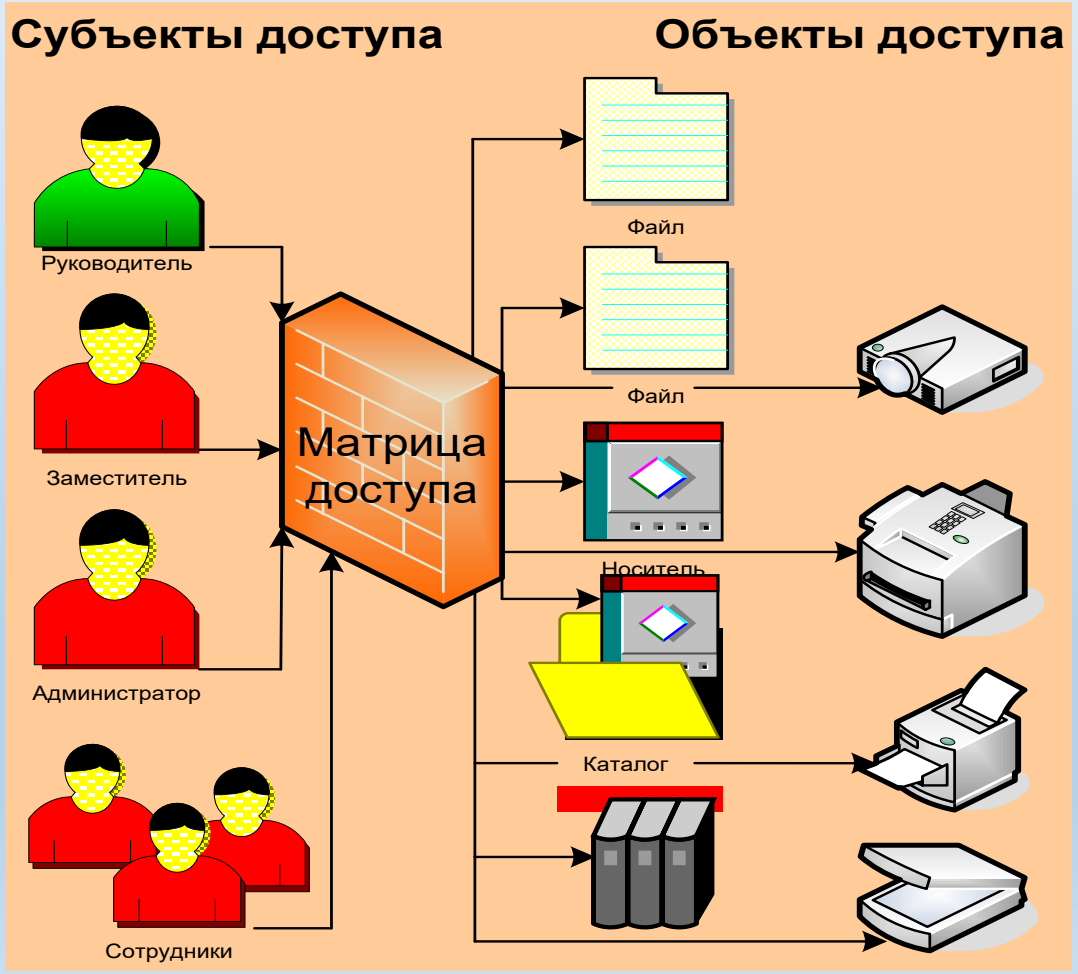
Субъект доступа - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Термины и определения

Дискреционная модель доступа

права доступа задаются матрицей доступа, элементами которой являются разрешенные права доступа субъекта к объекту



Термины и определения

Мандатная модель доступа

Каждому субъекту и каждому объекту ставятся в соответствие специальные классификационные метки.

Вывод:

- Количество инцидентов с **ПДн и КИИ** постоянно **увеличивается**.
- Сложность установления причин утечек, **умышленная или случайная**.
- Доля **случайных** утечек в организациях хоть и небольшая, но значительная.
- Снижение случайных утечек в коммерческих организациях **благодаря использованию SIEM-систем** (систем управления ИБ и событиями безопасности – обнаружение, анализ и устранение угроз безопасностис), **СКДПУ** (система контроля и отслеживания действий поставшиков ИТ-услуг).
- Возрастание **важности мер организационного**.
- **Особое место – необходимость в создании консультационно-образовательной среды по подготовке и консультационно-методической поддержки (КМП) персонала, ответственного за организацию защиты и обработку персональных данных и безопасную эксплуатацию КИИ.**
- **КМП** – это возможность проводить **консультации** и проверять **уровень подготовки** соответствующих специалистов, аттестовать их на соответствие квалификационным требованиям специалитета.
- **КМП** – возможность **текущего контроля** уровня подготовки персонала ответственного за обработку ПДн и иной информации ограниченного доступа

* В качестве примера – **Входной Тест** на знание основ ИБ, правил работы с информацией ограниченного доступа и НПА РФ в области ИБ

Контактная информация

МИНИСТЕРСТВО СВЯЗИ ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ

Отдел безопасности и спецсвязи

Абзалов Олег Накибович

Телефоны +7(949) 626-85-15

Сайт (раздел «Информационная безопасность»)

https://digital.gov-dpr.ru/deyatelnost/informatsionnaya-bezopasnost/

e-mail abzalov.on@digital.gov-dpr.ru

Ждем Ваших обращений!

Спасибо за внимание !